IN THE UNITED STATES DISTRICT COURT

FOR THE MIDDLE DISTRICT OF NORTH CAROLINA

In the Matter of the Search of A 2TB Hitachi Hard Drive Serial Number YFGNBBTA and Labeled HD-2	Case No: 1:18cr492 1:18mj307 **UNDER SEAL**

SUPPLEMENTAL PLEADING

NOW COMES the United States of America, by and through Matthew G.T. Martin, United States Attorney for the Middle District of North Carolina, and files a Supplemental Pleading as directed by the Court on March 19, 2019. Dkt. Ent. #17.

1. VeraCrypt is encryption software. It was used to prevent access to the data contained on a 2TB Hitachi hard drive recovered from the residence of the Defendant, Timothy Donovan BURNS. According to VeraCrypt's website (https://www.veracrypt.fr/en/Home.html), the software "is a free open source disk encryption software for Windows, Mac OSX and Linux. Brought to you by IDRIX (https://www.idrix.fr)." Attachment A, Graphic 1.

2. The Frequently Asked Questions (FAQ) portion of VeraCrypt's website (https://www.veracrypt.fr/en/FAQ.html), provides information about the software. This includes the following assertions:

- "What's the difference between TrueCrypt and VeraCrypt? VeraCrypt adds enhanced security to the algorithms used for system and partitions encryption making it immune to new developments in brute-force attacks. It also solves many vulnerabilities and security issues found in TrueCrypt." Attachment A, Graphic 2.
- **"I forgot my password – is there any way ('backdoor') to recover the files from my VeraCrypt volume?** We have not implemented any 'backdoor' in VeraCrypt (and will never implement any even if asked to do so by a government agency), because it would defeat the purpose of the software. VeraCrypt does not allow decryption of data without knowing the correct password or key. We cannot recover your data because we do not know and cannot determine the password you chose or the key you generated using VeraCrypt. The only way to recover your files is to try to "crack" the password or the key, but it could take thousands or millions of years (depending on the length and quality of the password or keyfiles, on the software/hardware performance, algorithms, and other factors)." Attachment A, Graphic 3.

3. A review of the IDRIX website (https://www.idrix.fr) reveals that IDRIX is based in Paris, France (https://www.idrix.fr/Root/mos/Contact_Us/task,view/contact_id,1/Itemid,30/). Attachment A, Graphic 4.

4. I have conferred with Dylan W. Greenwood, counsel for the Defendant, and he does not object to the Court taking judicial notice of the assertions on the VeraCrypt or IDRIX websites.

This the 27th day of March, 2019.

Respectfully submitted,

MATTHEW G.T. MARTIN
UNITED STATES ATTORNEY

/S/ ERIC L. IVERSON
Assistant United States Attorney
NCSB #46703
United States Attorney's Office
Middle District of North Carolina
101 S. Edgeworth St., 4th Flr.
Greensboro, NC 27401
Phone: 336/332-6302